AMENDMENTS TO THE CLAIMS

1-22 (Canceled)

23. (New) A method for encrypting and decrypting information comprising a string of symbols, said symbols included in an alphabet comprising a set of symbols, the method comprising the steps of:

generating a random sequence of values using a pseudo-random generator to provide a random value space, said pseudo-random generator being initialized, prior to providing said random sequence, by an initialization key comprising a string of numbers, said initialization key determining said random sequence to be provided by said pseudo-random generator such that subsequent initialization of said pseudo-random generator using the same initialization key will result in the same random sequence of values;

dividing said alphabet into a control alphabet comprising symbols designated not to be modified during encryption, and a message alphabet comprising symbols designated to be potentially modified during encryption, such that each of said symbols used to represent said information is included in either said control alphabet or said message alphabet, there being no symbol common to both said control alphabet and said message alphabet;

defining a mask alphabet comprising all or some of the elements in said random value space, the values in said random value space being numbers such that said mask alphabet comprises numbers;

performing a numbering of said message alphabet by assigning to each symbol of said message alphabet, with no omission or repetition, a number between 0 and N-1 to provide a number for each of said symbols, N representing the number of elements in said message alphabet, such that each symbol of said message alphabet is uniquely associated with a number between 0 and N-1;

assigning a permutation of said message alphabet to each element of said mask alphabet;

acquiring a primary encryption key comprising a string of numbers;

constructing said initialization key from all or part of said primary encryption key;

initializing said pseudo-random generator using said initialization key;

selecting a symbol from said information to be encrypted;

encrypting said selected symbol if it is determined that said selected symbol belongs to said message alphabet and performing the following steps:

reading the next value in said random sequence provided by said pseudo-random generator;

repeating the step of reading the next value until the next value read is an element of said mask alphabet to provide a mask element;

selecting permutation of said message alphabet assigned to said mask element;

applying said selected permutation of said message alphabet to said selected symbol to provide a result; and

replacing said selected symbol with said result of said selected permutation; and

repeating the steps of selecting a symbol and encrypting said selected symbol until all symbols from said information is selected.

24. (new) The method of claim 23, further comprising the step of decrypting said information by performing the following steps:

a) selecting a symbol from said information to be decrypted;

b) determining if said selected symbol belongs to said message alphabet;

reading the next value in said random sequence provided by said random generator;

c) repeating the step of reading the next value until said mask element is obtained;

d) selecting an inverse permutation of said permutation assigned to said mask element;

e) applying said selected inverse permutation to said selected symbol to provide a result;

f) replacing said selected symbol with said result of said selected inverse permutation;

repeating the steps a)-f) until all symbols from said information is decrypted.

25. (new) The method of claim 23, wherein the step of applying said selected permutation further comprises the steps of;

determining the number of said selected symbol;

adding said mask element to the number of said selected symbol to provide a modified symbol;

calculating a remainder by dividing said modified symbol by N; and

determining a symbol of said message alphabet whose number is said remainder, wherein said selected permutation corresponds to a modulo-N addition on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

26. (new) The method of claim 23, wherein the step of applying said selected permutation further comprises the steps of:

determining the number of said selected symbol;

subtracting said mask element from the number of said selected symbol to provide a modified symbol;

repeatedly adding, if it is determined said modified symbol is a negative number, the number N to said modified symbol until said modified symbol is a positive number;

calculating a remainder by dividing said modified symbol by N; and

determining a symbol of said message alphabet whose number is said remainder, wherein said selected permutation corresponds to a modulo-N subtraction on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

27. (new) The method of claim 23, wherein said mask alphabet comprises only non-zero numbers that are prime to N; and wherein the step of applying said selected permutation further comprises the steps of:

determining the number of said selected symbol;

multiplying the number of said selected symbol by said mask element to provide a modified symbol;

calculating a remainder by dividing said modified symbol by N; and

determining a symbol of said message alphabet whose number is said remainder, wherein said selected permutation corresponds to a modulo-N multiplication on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

28. (new) The method of claim 23, wherein said mask alphabet comprises only non-zero numbers that are prime to N; and wherein the step of applying said selected permutation further comprises the steps of:

determining the number of said selected symbol;

determining a number when multiplied by said mask element differs from the number of said selected symbol by a whole multiple of N to provide a first number;

calculating a remainder by dividing said first number by N; and

determining a symbol of said message alphabet whose number is said remainder, wherein said selected permutation corresponds to a modulo-N division on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

29. (new) The method of claim 23, wherein said mask alphabet comprises only non-zero numbers that are prime to Phi (N), where designates the number of integers between 1 and N-1 that are prime to N; and wherein the step of applying said selected permutation further comprises the steps of:

determining the number of said selected symbol;

calculating a remainder by dividing the number of said selected symbol raised to a power equal to said mask element by N; and

determining a symbol of said message alphabet whose number is said remainder, wherein said selected permutation corresponds to a modular exponentiation on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

30. (new) The method of claim 23, wherein said mask alphabet comprises only non-zero numbers that are prime to Phi (N), where designates the number of integers between 1 and N-1 that are prime to N; and wherein the step of applying said selected permutation further comprises the steps of:

determining the number of said selected symbol;

determining a positive number when raised to a power equal to said mask element differs from the number of said selected symbol by a whole multiple of N to provide a first number;

calculating a remainder by dividing said first number by N; and

determining a symbol of said message alphabet whose number is said remainder, wherein said selected permutation corresponds to a root extraction in modular arithmetic on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

31. (new) The method of claim 23, further comprising the step of associating each element of said mask alphabet with a quadruplet of numbers p, q, r and s, such that said number r and the result of the expression (p.s - q.r) are both non-zero numbers and are not multiples of N; and wherein the step of applying said selected permutation further comprises the steps of:

determining said quadruplet of numbers p, q, r and s associated said mask element;

determining a number m of a symbol to be encrypted or decrypted;

calculating a first result of the expression (m.r + s);

calculating, if it is determined that said first result is either zero or a multiple of N, a positive number k such that the expression (k.r – p) is a multiple of N;

calculating, if it is determined that said first number is neither zero nor a multiple of N, a positive number k such that the expression (k.(m.r + s) – (m.p + q)) is a multiple of N;

calculating a remainder by dividing said positive number k by N; and

determining a symbol of said mask alphabet whose number is said remainder, wherein said selected permutation corresponds to a homographic function in modular arithmetic on the symbol numbers such that said determined symbol is a result of said selected permutation being applied to said selected symbol.

32. (new) The method of claim 23, wherein said pseudo generator comprises a first pseudo-random generator and a hash algorithm; and further comprising the steps of:

initializing said first pseudo-random generator using said initialization key; and

providing said random sequence by said hash algorithm which uses the values provided by said first pseudo-random generator as an input data.

33. (new) The method of claim 23, wherein said pseudo generator comprises a first pseudo-random generator and an encryption algorithm; and further comprising the steps of:

constructing, from all or part of said primary encryption key, a secondary encryption key comprising a string of numbers;

initializing said first pseudo-random generator using said initialization key; and

encrypting the values provided by said first pseudo-random generator in accordance with said encryption algorithm using said secondary encryption key to provide said random sequence.

34. (new) A system, interposed between a client computer and a network comprising one or more other computers, for encrypting and decrypting information comprising a string of symbols, said symbols included in an alphabet comprising a set of symbols, said alphabet being divided into a control alphabet comprising symbols designated not to be modified during encryption and a message alphabet comprising symbols designated to be potentially modified during encryption, each symbol belonging to said message alphabet being previously associated with a number between 0 and N-1 to provide a number for each of said symbols, N designating the number of elements in said message alphabet, such that each symbol of said message alphabet is uniquely associated with a number between 0 and N-1, the system comprising:

a pseudo-random generator for generating a random sequence of values or numbers to provide a random value space, a subset of said random value space forming a mask alphabet, said pseudo-random generator being initialized prior to utilization with an initialization key comprising a string of numbers, said initialization key determining said random sequence that will be provided by said pseudo-random generator;

an input-output unit for handling communications among the system, said client computer and said network; and

a processor for:

acquiring a primary encryption key comprising a string of numbers and constructing said initialization key from all or part of said primary encryption key;

determining whether a value belonging to said random value space belongs to said mask alphabet;

reading successive values provided by said pseudo-random generator until an element belonging to said mask alphabet is obtained;

determining which of said symbols of said information must be encrypted or decrypted, and which of said symbols of said information must be transmitted without being modified;

associating a number with a symbol of said message alphabet;

selecting a mask element from a given element of said the mask alphabet and a permutation of said message alphabet which is assigned to said mask element; and

determining a result of applying said selected permutation to said given element provided by said input-output unit and transmitting said result to said input-output unit.

35. (new) The system of claim 34, wherein said input-output unit comprises:

a first input-output unit for handling communications between the system and said client computer; and

a second input-output unit for handling communications between the system and said network.

36. (new) The system of claim 34, wherein said processor is operable to select an inverse permutation of said permutation assigned to said mask element.

37. (new) The system of claim 34, wherein said processor is operable to perform an addition in modular arithmetic between said number associated with a symbol of said message alphabet and said mask element, and associate the result of said addition with an element of said message alphabet.

38. (new) The system of claim 34, wherein said processor is operable said to perform a subtraction in modular arithmetic between said number associated with a symbol of said message alphabet and said mask element, and associate the result of said subtraction with an element of said message alphabet.

39. (new) The system of claim 34, wherein said processor is operable to perform a multiplication in modular arithmetic between said number associated with a symbol of said message alphabet and said mask element, and associate the result of said multiplication with an element of the message alphabet.

40. (new) The system of claim 34, wherein said processor is operable to perform a division in modular arithmetic between said number associated with a symbol of said message alphabet and said mask element, and associate the result of said division with an element of said message alphabet.

41. (new) The system of claim 34, wherein said processor is operable to perform an exponentiation in modular arithmetic of said number associated with a symbol of said message alphabet, with said mask element as the exponent, and to associate the result of said exponentiation with an element of said message alphabet.

42. (new) The system of claim 34, wherein said processor is operable to perform a root extraction in modular arithmetic, and associate the result of said root extraction with an element of said message alphabet.

43. (new) The system of claim 34, wherein said message alphabet comprises N number of symbols; and wherein said processor is operable to:

associate said mask element with a quadruplet of numbers noted p, q, r and s;

associate a symbol of said message alphabet with a number m between 0 and N-1;

calculate the expression (m.r + s);

determine whether the expression (m.r + s) is zero or a multiple of N;

calculate a number k between 0 and N-1 such that the expressions (k.r – p) and (k.(m.r + s) – (m.p + q)) are multiple of N; and

associate said number k with an element of the message alphabet.

44. (new) The system of claim 34, wherein said pseudo-random generator comprises:

a first pseudo-random generator which is initialized using said initialization key and

a calculating means for applying a hash algorithm to the values provided by said first pseudo-random generator and transmitting the result of said hash algorithm to said processor.

45. (new) The system of claim 34, wherein said processor is operable to construct, from all or part of said primary encryption key, a secondary encryption key comprising a string of numbers; and wherein said pseudo-random generator comprises:

a first pseudo-random generator which is initialized using said initialization key and

a calculating means for applying an encryption algorithm to the values provided by said first pseudo-random generator and transmitting the result of said encryption algorithm to said processor.

46. (new) The system of claim 34, wherein said processor comprises one or more processors to perform various tasks of said processor.